

The complaint

Mr M complains about Revolut Ltd.

He says that Revolut didn't do enough to protect him when he became the victim of a scam and would like Revolut to refund him the money he has lost as a result.

What happened

Mr M unfortunately fell victim to a cryptocurrency investment scam. The scam began when Mr M received a message from an individual through an app who said that they were making money via cryptocurrency, and that Mr M could do the same.

Under direction from the individual, Mr M opened an account with a well-known crypto exchange. Mr M then moved money from his account with N to Revolut, and from here to the crypto exchange. Mr M believed the funds were then added to his own trading portal – but this was a fabrication – and the money was lost when it was transferred from one crypto wallet to another.

Mr M made the following payments from his account with Revolut.

Payment	Date	Payment type	Amount
1	14/06/2023	Card to B (crypto exchange)	£500
2	14/06/2023	Card to B (crypto exchange)	£5,000
3	15/06/2023	Card to B (crypto exchange)	£2,500
4	26/06/2023	Card to B (crypto exchange)	£5,000
5	27/06/2023	Card to B (crypto exchange)	£820
6	04/01/2024	Card to B (crypto exchange)	£50
7	04/01/2024	Card to B (crypto exchange)	£100
8	05/01/2024	Card to B (crypto exchange)	£51
9	05/01/2024	Card to B (crypto exchange)	£100
10	06/01/2024	Card to B (crypto exchange)	£2,000
11	08/01/2024	Card to B (crypto exchange)	£1,880
		Total	£18,001

However, when he attempted to make a withdrawal, he was unable to do so, and realised he had been the victim of a scam.

Mr M then made complaints to N and Revolut, but neither business upheld his complaint.

Our Investigator looked into things and thought that N should refund Mr M 50% of the first £5,500 Mr M moved from his account with it, and then liability for the remaining loss from payment three onwards should be shared between N, Mr M and Revolut.

Revolut disagreed and asked for a final decision to be made on the complaint Mr M brought against it – so as both complaints are inextricably linked, I will be issuing a final decision on both complaints.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in *Philipp v Barclays Bank UK PLC*, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In *Philipp*, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Mr M modified the starting position described in *Philipp*, by – among other things – expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*" (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks. In practice Revolut did in some instances, refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider

to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in June 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;¹
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

For example, it is my understanding that in June 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)².
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms"*.
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to

¹ For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks/

² Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code³, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.
- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So, it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in June 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and

³ BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in June 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Mr M was at risk of financial harm from fraud?

It isn't in dispute that Mr M has fallen victim to a cruel scam here, nor that he authorised the payments to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer). I have set out in this decision the circumstances which led Mr M to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster.

Revolut has argued that as Mr M's account was dormant, it didn't know what the typical account usage would be for Mr M – and it pointed out that the account was opened with the purpose of making transfers and cryptocurrency. However, I believe that Revolut should have known that something was amiss – and that Mr M may have been at risk of financial harm.

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that these payments would be credited to a cryptocurrency wallet held in Mr M's name

By June 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr M made, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting as Revolut argues that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks. Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Mr M's own name should have led Revolut to believe there wasn't a risk of fraud.

So, I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr M might be at a heightened risk of fraud that merited its intervention.

While the first payment Mr M made to the scammer was small, the second payment was much larger, but I am mindful that Mr M had told Revolut that one of the purposes of opening his account was to make crypto purchases. On balance, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, I don't think Revolut ought to have been sufficiently concerned about this payment that it would be fair and reasonable to expect it to have provided warnings to Mr M at this point.

However, when the third payment was made, Mr M had made payments to crypto of £8,000 within 24 hours and had credited his previously dormant account with over £13,500. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr M was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead. To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by June 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its

services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

However, Revolut did not provide any warnings to Mr M about any of the payments he made.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to the ones Mr M was making will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, when Mr M made his third Payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value. I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mr M by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr M suffered from the third payment?

Mr M has previously shown that when questioned about the payments he was making, he did not hide any details, or ignore any warnings provided to him – so I think that had Revolut done as I would have expected, it would have quickly identified that he was at risk of a common type of scam and provided him with a warning about what he was doing to that effect.

I think that a warning provided by Revolut would have given the perspective Mr M would have needed to identify that he was at risk – and I don't think that Mr M would have ignored such a warning either.

So, I think it is unlikely he would have continued with the payment, had this warning been given to him.

Is it fair and reasonable for Revolut to be held responsible for Mr M's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr M purchased cryptocurrency which credited an e-wallet likely held in his own name, rather than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost to the fraudsters. I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr M might have been at risk of financial harm from fraud when he made the third Payment, and in those circumstances, it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Mr M suffered. The fact that the money used to fund the scam came from elsewhere does not alter that fact and I think Revolut can fairly be held responsible for Mr M's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

As I have previously explained, Mr M has made two complaints to this Service about the scam he fell victim to – and I have considered both simultaneously – which is reflected in the redress I have recommended.

Should Mr M bear any responsibility for their losses?

Having thought about this carefully, I do think that Mr M wasn't as careful as he should have been before parting with his money. He received an unsolicited message about a crypto investment and received no paperwork in relation to his supposed investment. Additionally, while Mr M says that he went online to look into the company he thought he was investing in, and found no negative reviews, there was information available at the time that suggested that there was a high risk associated with the app Mr M downloaded. I also think that the returns Mr M was told he could achieve were unrealistic and should have given him cause to think that they were too good to be true.

As I have previously explained, Mr M has also brought a separate complaint against N to this Service – which I have also considered and upheld in part. Where multiple banks, and the consumer themselves could have done more, I think it would be fair for them all to bear some responsibility for the loss.

Putting things right

Revolut Ltd should refund Mr M 33% of payment three onwards.

On top of this, it should also pay Mr M 8% simple interest from the date the payments were made until settlement (less any lawfully deductible tax).

My final decision

I uphold this complain in part. Revolut Ltd should put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 10 January 2025.

Claire Pugh
Ombudsman